DEPARTMENT OF THE TREASURY

FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF TRAINING

FINANCIAL FRAUD INSTITUTE

SYLLABUS

CRIMINAL INVESTIGATIONS IN AN AUTOMATED ENVIRONMENT TRAINING PROGRAM (CIAETP)

SEPTEMBER 2002

CRIMINAL INVESTIGATIONS IN AN AUTOMATED ENVIRONMENT TRAINING PROGRAM TABLE OF CONTENTS

HISTORY AND PURPOSE of the Criminal Investigations in an Automated Environment Training Program (CIAETP)

Crimes against society are not limited to city streets and alleys but are found just as frequently in the sanitized corridors of corporate offices and computer rooms. The Federal Law Enforcement Training Center (FLETC) and its participating organizations recognized that, because of the evolution of computer technology and its impact on so many areas of our society, a vacuum existed in the training of Federal investigators in the detection and investigation of computer fraud and abuse. In order to fill this void, the FLETC, with the vigorous support of its participating organizations, initiated the development of the Computer Fraud and Data Processing Investigations Training Program (CFDPITP) in December 1982.

Between January 1984 and October 1988, CFDPITP trained over 600 Federal and state and local law enforcement officers in the investigation of computer related crimes. The objectives of the program were varied: to introduce the concept of data processing technology to non-computer professionals; to discuss the methodologies of computer crime as well as effective investigative techniques; to present up-to-date legal principles relating to computer generated evidence and search and seizure, to discuss preventative measures of computer related fraud and abuse. Extensive hands-on training was provided and class size was limited to allow for maximum participation in this intensive training program.

Several factors prompted the FLETC to reevaluate the efficacy of CFDPITP. The evolving nature of computer related crime resulted in fewer occurrences of "pure" computer fraud for agents to investigate, while there appeared far more instances of criminal cases in which the computer acted as a tool for the facilitation of a wide variety of criminal activity, such as contract fraud, money laundering, and similar offenses. Additionally, microcomputers were perceived as having a growing impact on modern business and government environments, "hacking" and other instances of telecommunications crimes were seen as proliferating, and these categories of abuse were not being addressed.

In January 1988, the FLETC hosted a Curriculum Review Conference to discuss the modification and up-dating of CFDPITP. Over 20 organizations, from Federal and state and local agencies, were represented in the conference. The consensus of the conference participants was that the objectives of the program should be expanded to reflect current trends in technology-related crimes, and that, since basic computer training was provided by other organizations and programs, all introductory courses should be eliminated. The recommendations of the conference were approved by the Director and the name was changed to Criminal Investigations in an Automated Environment Training Program (CIAETP) to more accurately reflect the nature of the program. The program is directed primarily toward financial crime investigators (as well as criminal investigators not involved directly in financial investigations) who have a working knowledge of computers and data processing (this working knowledge will be defined later). However, the training program is also open to certain non-investigators who routinely work as part of the investigative team. Instruction is provided by experienced criminal investigators, data processing professionals, and attorneys knowledgeable in the field of computer law.

In September 1993, the FLETC hosted a Curriculum Review Conference for the Basic Microcomputer Training Program (BMCTP), the Advanced Microcomputer Training Program (AMCTP) and the Criminal Investigations in an Automated Environment Training Program (CIAETP). It was decided that the BMCTP and AMCTP would be combined into the Microcomputers for Investigations Training Program (MITP), and should be a prerequisite for the CIAETP. Regarding the CIAETP, it was concluded that it should include more technical information, and less introductory information about using the computer as an investigative tool. Criminal Investigators and Police Officers of the 90's are aware of the importance of computer usage during the course of an investigation, and many are aware of the basic concepts governing the involvement of computers as the storehouse of evidence, tools/instruments of crime, and as the fruits of criminal activity. More time needed to be spent on the policies and procedures used when seizing computer systems, on the legal issues that have an impact on the seizure of computer systems, and on the subsequent investigative analysis of computer systems. The CIAETP has evolved to meet advancing technological strategies in the law enforcement environment.

The FLETC and the Financial Fraud Institute (FFI) are committed to bringing together criminal investigator participants from a variety of law enforcement agencies and to provide the opportunity for sharing skills and experience in the rapidly evolving field of technology related investigations. Finally, the FLETC aims to make all those actively involved in the computer/financial crime investigatory process aware of the wealth of talent available within the Federal and state and local services which can be united in purpose to detect, investigate, and prosecute these crimes.

ADMINISTRATION

Applicants should telephone the FLETC Scheduling and Allocation Division at (912) 267-2421 or (912) 267-2580 for enrollment information. Upon acceptance in a program, a confirmation letter with details on housing, transportation, and schedule will be mailed to the participant.

All training participants will report to the classroom by 7:30 a.m. on the first day of training. They should check in at the FLETC on the previous evening. The FLETC reserves the right to deny participation to anyone with an unexcused late arrival.

Length of Program

The training program encompasses 2 weeks (80 Hours), beginning on a Monday and ending on the second Friday, with the graduation scheduled at approximately 11:00 to 11:30 a.m.

Standard Daily Schedule (Approximately)

Morning session(s)	7:30 to 11:30 a.m.
Lunch	11:30 a.m. to 12:30 p.m.
Afternoon session(s)	12:30 to 4:30 p.m.

Depending on the level of knowledge of students, the program coordinator does reserve the right to schedule mandatory after hours training to bring students' knowledge up to the level expected for attendance to this training program.

On the last day of scheduled training, the program will conclude at approximately 11:00 a.m. Due to FLETC transportation requirements, no airline departure should be scheduled earlier than 2:00 p.m. The FLETC reserves the right to deny graduation for any student departing prior to the end of the graduation.

Program Cost

Fees cover all costs including room, board and supplies. These supplies include approximately 20 diskettes for participants to use to make copies of investigative utilities for use during investigative disk analysis. Participants are responsible for their own transportation expenses to the FLETC. Since costs vary from year to year, the participation fees for programs are listed in the annual schedule of classes.

Location

All training is conducted at the FLETC, Glynco, Georgia, an interagency training facility located 6 miles north of Brunswick, Georgia, and approximately 75 miles equidistant from Jacksonville, Florida, and Savannah, Georgia. The FLETC is located near the beach resorts of St. Simons Island, Sea Island and Jekyll Island, Georgia. The climate is moderate and lends itself to year-round training.

Photograph/Dress Code

On the third day of the training program, a Class Photograph will be taken. All students are required to be in the photograph, but are not required to purchase the photograph. The cost of the photograph *is not included* in any fees paid to FLETC. Students should bring clothing appropriate for a class photograph (i.e. jacket/tie for males, suit/dress for females).

Other than when the class photograph is taken, the dress code for class is business casual: collared shirt/slacks (No jeans, shorts, or T-shirts).

Qualifications for Admission

The FLETC Board of Directors has determined that this training program is available to participating Federal organizations actively involved in investigating crimes in which the computer may play an active or passive role. Other Federal, state or local agencies may attend on a space-available basis.

The participant should be a Criminal Investigator who has graduated from the FLETC basic Criminal Investigator Training Program (or an equivalent training academy). It is expected that the training participant will be an experienced investigator with a practical knowledge of, and experience in, criminal law, Federal Court Procedures, and other investigations related areas. However, the training program is also open to certain non-investigators who routinely work as part of the investigative team.

A functional knowledge of microcomputers is required. More specifically, this means:

1. Experience with the majority of the functions of a Word Processor.

2. Exposure to the concepts governing the use of an Electronic Spreadsheet (i.e. What is a cell, and what are formulas?) and a Database Manager (i.e. How may a query be phrased, and what do AND and OR mean in a query statement?)

3. Training or background in the use of a mouse, and knowledge of the basic concepts governing the use of Microsoft Windows, version 3.1 or Windows 95.

4. Use of a DOS or Windows 95 microcomputer NOT FROM A MENU!!! In other words, from the command/system prompt. Students must possess knowledge of the usage of basic DOS commands, including, but not limited to:

   DIR
   Create "Subdirectories" on a diskette/hard disk (MD) and store data within the subdirectories; also access the subdirectories (CD), and remove the subdirectories (RD).
   FORMAT
   COPY one file/many files/entire diskettes
   DEL/ERASE one file/many files
   TYPE to view the contents of Text Files, |MORE to page the display

5. Knowledge of the importance of the AUTOEXEC.BAT and CONFIG.SYS files and what, in general, Batch files are.

6. How to recognize a computer program file from a "Directory" listing of files on a diskette/hard disk.

7. Knowledge and application of the differences between different "densities" of diskettes and diskette drives.

Successful completion of FLETC's Microcomputer for Investigations Training Program (MITP) is required for admission to the CIAETP. Applicants that have not attended FLETC's MITP may attend the Criminal Investigations in an Automated Environment (CIAETP) if they have experience and knowledge, acquired through formal education or on-the-job training, which is equivalent to what is presented within the MITP. Potential students in this situation must pass a pretest before attending the training program. When they register or are registered for the training program, they should be told to contact the program coordinator. The program coordinator will send them the pretest, which must be returned prior to their attendance to the training program. Students that do not pass the pretest will not be allowed to attend the CIAETP.

Student Evaluation

In order to satisfy all requirements for graduation from the CIAETP and receive a graduation certificate, training participants must accomplish the following:

Attendance: Training participants must be present for every class presented within the CIAETP. Any emergencies that surface during the training program requiring student absence from class must be discussed with the Program Coordinator and the Program Manager. Court appearances or other job related absences will not excuse students from class. An unexcused absence from class will result in failure to graduate from the training program; a letter of attendance will be sent in lieu of a graduation certificate.

Practical Exercises: The CIAETP is a progressive training program. Each student must successfully complete the practical exercises for one course in order to proceed to the next course. The final practical exercises involves an investigative scenario which tests all objectives in the training program. Training participants will successfully complete the training program by completing the following practical exercises:

1. Locate data on a diskette based on an investigative scenario using DOS, Batch File Concepts, Windows and File Viewers.

2. Locate erased data on a diskette based on an investigative scenario using various Utility computer programs.

3. Pursuant to the Case Investigation Scenario: Discuss and develop probable cause and an affidavit to execute a search warrant directed toward computer equipment.

4. Pursuant to the Case Investigation Scenario: Develop an investigative plan to execute a search warrant directed toward computer equipment, including methods to secure computer systems and conduct backups.

5. Pursuant to the Case Investigation Scenario: Execute the search warrant and appropriately secure and back up computer hard disks at the search site, maintaining the authenticity and integrity of the evidence. Seize and transport authorized items back to "office."

6. Pursuant to the Case Investigation Scenario: Appropriately prepare classroom computer systems to accept restoration of seized data based on it's original configuration.

7. Pursuant to the Case Investigation Scenario: Analyze seized magnetic media, including restored computer system hard disk data and diskettes.

8. Pursuant to the Case Investigation Scenario: Prepare to present case to a United States Attorney, including precautions taken to maintain integrity of the computer evidence, and technical methods used to recover information.

ADDITIONAL INFORMATION

Additional information concerning the Criminal Investigations in an Automated Environment Training Program (CIAETP) may be obtained by contacting:

Federal Applicants

CIAETP Program Coordinator (912) 267-2314
Financial Fraud Institute (912) 267-2500 (fax)
Bldg. 210
Federal Law Enforcement Training Center
Glynco, GA 31524

State/Local Applicants

Director
Federal Law Enforcement Training Center
Office of State/Local Training
Glynco, GA 31524

(912) 267-2345
(800) 743-5382

PARTICIPATING AGENCIES

The following are the participating agencies at the Federal Law Enforcement Training Center (FLETC):

EXECUTIVE BRANCH

AGRICULTURE
- Forest Service

COMMERCE
- National Institute of Standards and Technology
- National Marine Fisheries Service
- Office of Security
- Office of Export Enforcement

DEFENSE
- Defense Protective Service
- Naval Criminal Investigative Service
- National Security Agency

HEALTH AND HUMAN SERVICES
- Food and Drug Administration
- National Institutes of Health

INTERIOR
- Bureau of Indian Affairs
- Bureau of Land Management
- Bureau of Reclamation
- National Park Service
- Office of Surface Mining, Reclamation and Enforcement
- U.S. Fish and Wildlife Service

JUSTICE
- Bureau of Prisons
- Drug Enforcement Administration
- Immigration and Naturalization Service
- U.S. Marshals Service

STATE
- Bureau of Diplomatic Security

TRANSPORTATION
- Federal Aviation Administration
- U.S. Coast Guard

TREASURY

- Bureau of Alcohol, Tobacco and Firearms
- Bureau of Engraving and Printing
- Financial Crimes Enforcement Network (FinCEN)
- Internal Revenue Service
- U.S. Customs Service
- U.S. Mint
- U.S. Secret Service

PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY

Inspector General Offices:

- Agency for International Development
- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of Housing and Urban Development
- Department of Interior
- Department of Justice
- Department of Labor
- Department of State
- Department of Transportation
- Department of the Treasury
- Environmental Protection Agency
- Federal Deposit Insurance Corporation
- Federal Emergency Management Agency
- General Services Administration
- Government Printing Office
- National Aeronautics and Space Administration
- Nuclear Regulatory Commission
- Office of Personnel Management
- Railroad Retirement Board
- Resolution Trust Corporation
- Small Business Administration
- Social Security Administration
- United States Information Agency
- Veterans Administration

LEGISLATIVE BRANCH

CONGRESS

- Government Printing Office
- Library of Congress Police

U.S. Capital Police

JUDICIAL BRANCH

SUPREME COURT
Supreme Court Police

INDEPENDENT

AMTRAK
Northeast Corridor Police

CENTRAL INTELLIGENCE AGENCY
Office of Security

ENVIRONMENTAL PROTECTION AGENCY
Office of Criminal Investigations

FEDERAL EMERGENCY MANAGEMENT AGENCY
Security Division

GENERAL SERVICES ADMINISTRATION
Office of Federal Protective Service

SMITHSONIAN
National Zoological Park
Office of Protection Service

TENNESSEE VALLEY AUTHORITY
Office of the Inspector General
Public Safety Service

U.S. POSTAL SERVICE
Postal Inspection Service - Postal Police

PROGRAM SUMMARY

The Criminal Investigations in an Automated Environment Training Program (CIAETP) is an interagency program developed by the FLETC in coordination with representatives of several Federal and state and local agencies. The purpose of the program is to acquaint criminal investigators with the fundamentals of investigative procedures in a computer environment and to provide criminal investigators (or those that routinely serve as part of the investigative team) with the ability to analyze magnetic media seized pursuant to the execution of a search warrant.

The 2-week CIAETP is sequential in construction. That is, the information obtained in a particular course or practical exercise serves as a foundation for subsequent classes and exercises. Technical, legal and investigative subjects are interspersed equally throughout the CIAETP.

The CIAETP participants use the most current speed IBM compatible microcomputers and Hewlett-Packard Laser printers. Microcomputer software stored on the computer systems include MS-DOS and Windows 3.1, as well as Windows 95, Quickview 3.0 file viewer, Microsoft Office Professional, including Word, Excel, Access and Powerpoint, WordPerfect for Windows, Norton Utilities, and several other commercial, non-commercial and proprietary packages. Students also use external Zip and Jaz drives during practical exercises.

Students are allowed to check out laptop/notebook computers for use after hours to complete homework and class assignments.

Course instruction is primarily the responsibility of the Financial Fraud Institute, with two courses presented by the Legal Division of the FLETC. In addition, guest lecturers from several Federal and state and local agencies are used to augment FLETC instruction.

The training program includes a series of several practical exercises used for evaluation purposes. The final practical exercises are constructed around an investigative scenario, which has been designed to provide as much realism as possible in a training environment. All situations contained in the exercises are gleaned from actual investigations, although contexts and names have been altered for training purposes.

The course descriptions and objectives listed herein are presented in this format: course title, length and method of presentation, description, objectives, and method of evaluation. The length of the courses is presented in hour and minute notations.

Three methods of presentation are listed with this format. These are:

Lecture/Classroom- A training situation, indoors or outdoors, in which instructional material is being presented by an instructor.

Laboratory- A training situation, indoors or outdoors, in which students are practicing skills under the guidance of an instructor(s).

Practical Exercises- A training situation, indoors or outdoors, in which students, under the supervision or evaluation of an instructor(s), are participating in a law enforcement related activity which will be graded.

OBJECTIVES:

At the conclusion of this two week program, the training participant will have demonstrated, through the successful completion of several practical exercises and a case study, that they have a functional knowledge of:

-- Relation of traditional legal, evidentiary and seizure practices to automated environments;

-- Techniques of computer related crime and its detection by the law enforcement officer;

-- General investigative techniques used when executing a search warrant in an automated environment;

-- Methods used to recover hidden/erased/disguised data from seized diskettes or other magnetic media on various IBM compatible microcomputer systems;

-- Appropriate procedures used to safely access data on a seized IBM-compatible computer system while maintaining the authenticity and integrity of the evidence;

-- Strategies used to backup and restore seized computer data on IBM-compatible computer systems.

These objectives will be addressed through lecture, discussion, various types of practical exercise involving investigative scenarios, and demonstrations of relevant techniques.

PROGRAM OF INSTRUCTION

Criminal Investigations in an Automated Environment
Training Program
(CIAETP)

COURSE TITLE: DISK ANALYSIS: DOS/BATCH FILES (3232.06)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
2:00	2:00	2:00	6:00

DESCRIPTION:

This course begins a series of courses intended to teach the participant how to perform an investigative analysis on a diskette or on a hard disk seized pursuant to the execution of a search warrant. Students begin by establishing steps to take before the diskette/hard disk is analyzed, then move toward defining and using the DOS programs to examine and view data on a seized diskette or hard disk.

TERMINAL PERFORMANCE OBJECTIVE:

Given an IBM compatible computer system and a seized diskette or seized computer system with a hard disk, perform an investigative analysis of the seized data using DOS programs and extract information of importance within various investigative scenarios.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify steps taken and programs run before analyzing data on a seized diskette.

2. Identify and use various DOS programs to examine and view data on a seized diskette or hard disk.

3. Identify and use DOS programs that can adversely affect the investigative analysis of computer systems at the search site.

4. Identify general principles governing batch files and read/interpret batch files to determine what they have been programmed to do to data stored on seized computer systems.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: DISK ANALYSIS: Microsoft Windows and File Viewers (3231.04)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
:30	1:30	2:00	4:00

DESCRIPTION:

Investigators and special agents involved in virtually any type of investigation today must be computer literate in order to do their jobs properly. During the course of their investigations, many law enforcement officers acquire data that is either already stored on magnetic media or that must be stored on magnetic media in order to be most efficiently analyzed via computer. Many law enforcement officers have computer systems on their desks using Microsoft Windows 3.1. Also, many of the computer systems being seized from homes and small businesses are running Windows 3.1. Knowledge of the operations of this computer program would be extremely helpful to any law enforcement officer in the seizure and analysis of computer systems.

This course is divided into two phases, one of which is dependent on the prior knowledge of the participants. The first phase involves the introduction of concepts governing the use of Microsoft Windows from a user perspective, including the use of the Main (File Manager), Accessories, and Applications windows. The second phase is an analytical look at Microsoft Windows, including the examination of the Clipboard, INI files, passwords, swap files, and other areas of importance to the investigator. The first phase is scheduled for two hours after the normal class day on day 1 of the training program, and is mandatory for those not familiar with the topics listed in the objectives. The second phase is scheduled during the normal class day afternoon on day 2 of the training program.

TERMINAL PERFORMANCE OBJECTIVE:

Given an IBM compatible computer system with Microsoft Windows and associated file viewer applications, view program and data files seized pursuant to an investigative scenario and locate relevant investigative information using various Windows information files.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify several reasons for the popularity of Microsoft Windows.

2. Identify the components of a Windows screen and describe the function of each of the following:

a. Buttons, bars and arrows
b. Windows pull-down menu options
c. Icons
d. Maximizing and Minimizing; Difference between minimizing and closing.

3. Use the DOS Shell to temporarily exit out of Windows to perform a DOS operation, and correctly reenter Windows.

4. Identify the icons in the Main and Accessories Groups, which are programs provided with Windows.

5. Manipulate the Windows "groups" and "items" by creating, modifying, moving and deleting groups and items.

6. Identify the major .INI files used by Windows during a typical session and their functions.

7. Use methods to disable the password feature enabled through the screen saver feature through CONTROL.INI.

8. Use methods to determine what programs are defined as icons through Windows without running the Windows program.

9. Identify areas that may be good sources of information during an investigative analysis of a computer system using Windows 3.1 as its program menu shell.

10. Use the Quick-View File Viewer to view program and data files pursuant to an investigative scenario.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: DISK ANALYSIS: DOS/BATCH FILES AND WINDOWS/FILE VIEWERS PRACTICAL EXERCISE (3218.02)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
		2:00	2:00

DESCRIPTION:

This course is a comprehensive practical exercise which evaluates material covered within two courses: Disk Analysis: DOS/Batch Files and Disk Analysis: Windows/File Viewers. These courses taught the participant how to perform an investigative disk analysis using DOS commands and Windows File Viewers, and how to view and analyze batch files. Participants will perform an investigative analysis on a diskette based on an investigative scenario. Participants will be required to turn in an investigative analysis plan, a list of what they find, as well as how they found it.

TERMINAL PERFORMANCE OBJECTIVE:

Given an IBM compatible computer system and a seized diskette under an investigative scenario, perform an investigative analysis of the seized data using DOS programs, knowledge of batch files and Windows file viewers and extract information of importance.

INTERIM PERFORMANCE OBJECTIVES:

1. Create an investigative disk analysis plan.

2. Document steps taken during an investigative analysis of a seized diskette.

3. Use various DOS programs and knowledge of batch files to examine and view data on a seized diskette pursuant to an investigative scenario.

4. Use Windows file viewers to read and interpret files such as spreadsheets, databases and graphics files, that cannot be read from the DOS prompt pursuant to an investigative scenario.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: DISK ANALYSIS: Boot-up Process and Configuring a Boot Disk (3229.04)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
2:00	1:00	1:00	4:00

DESCRIPTION:

In utilizing or investigating an IBM compatible microcomputer system, knowledge of MS-DOS commands and batch file operation is important, but it is also vital to understand the internal operations of the microcomputer and how it stores the programs that are executed. This course describes the components of the operating system, what happens when the microcomputer is activated, and explains how to interpret many of the commands in the CONFIG.SYS and AUTOEXEC.BAT files. This course also discusses how to create a boot disk for use during the execution of a search warrant.

TERMINAL PERFORMANCE OBJECTIVE:

Given a seized IBM compatible microcomputer during a final practical exercise, and printouts of configuration files from other IBM compatible microcomputers, the student will analyze the contents of CONFIG.SYS and AUTOEXEC.BAT files, and will create a boot diskette to be used during the Execution of a Search Warrant practical exercise and subsequent analysis of the seized computer system.

INTERIM PERFORMANCE OBJECTIVES:

1. Describe the three characteristics of all Operating systems and problems that may occur when files are mixed between different versions of operating systems.

2. Describe the procedures performed by a typical IBM compatible microcomputer when it is activated, and the contents of typical CONFIG.SYS and AUTOEXEC.BAT files.

3. Create a boot disk to be used to secure seized computer equipment for transportation.

METHOD OF EVALUATION: Demonstrated proficiency..

COURSE TITLE: DISK ANALYSIS: Recovering Erased Data from Disks (3228.18)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
4:00	6:00	8:00	18:00

DESCRIPTION:

This is the last of the four courses on techniques used to analyze a diskette or computer system's hard disk data seized pursuant to an investigation. The first three courses focused mainly on DOS programs and other applications that are based on DOS's rules and regulations. This course concentrates on the more complicated techniques used to recover erased and hidden data from disks and diskettes. During practical exercises, students use information from several investigative scenarios to recover pertinent information from diskettes. During a final practical exercise, students use information received within the context of the Continuing Case Investigation to recover information from diskettes and from a seized computer system's hard disk.

TERMINAL PERFORMANCE OBJECTIVE:

Given an investigative scenario(s) and an IBM compatible Microcomputer, the student will recover erased and concealed data from a diskette.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify the difference between the formatting process on a diskette for DOS 4.0 and before and DOS 5.0 and after, and how this affects the investigative analysis of a diskette.

2. Identify what happens when a hard disk is "partitioned" and how the partition information may be manipulated to disguise data from an investigative analysis.

3. Define the major techniques used to manipulate a seized diskette or computer system's hard disk directory entries to conceal data and use these methods to retrieve concealed data.

4. List the steps performed by MS-DOS when data is stored on and erased from a diskette and employ this information to recover erased data from a seized diskette or computer system's hard disk.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: DISK ANALYSIS: Final Practical Exercise (3233.04)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
		5:00	5:00

DESCRIPTION:

This practical exercise is comprehensive and encompasses several courses presented during the training program. The information is introduced to students prior to and is a direct result of the Execution of a Search Warrant Practical Exercise. During the Execution of a Search Warrant practical exercise, students are required to backup the computer systems at the search site using appropriate hardware and software. Students then must analyze the data during this practical exercise to discover information relevant to the investigation. Students must configure classroom computer systems appropriately and restore backups to these computer systems. Students must also prepare for presentation of their case and the information discovered during analysis of the seized data to an attorney.

TERMINAL PERFORMANCE OBJECTIVE:

Given diskettes and computer data seized pursuant to an investigative scenario, perform an investigative analysis of the seized data.

INTERIM PERFORMANCE OBJECTIVES:

1. Appropriately configure computer system hard disks for restoration of seized computer data backed up at the search site.

2. Restore seized computer data to computer systems.

3. Create an investigative disk analysis plan.

4. Document steps taken during an investigative analysis of a seized diskette or hard disk.

5. Use various DOS programs and knowledge of batch files to examine and view data on a seized diskette pursuant to an investigative scenario.

6. Use Windows file viewers to read and interpret files such as spreadsheets, databases and graphics files, that cannot be read from the DOS prompt pursuant to an investigative scenario.

7. Locate data on hard disks associated with files with manipulated attributes.

8. Locate erased files and use a computer program to unerase the files.

9. Find data once associated with erased and partially overwritten files and recover the data.

10. Present information discovered during analysis and case information to an attorney.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Computer Search and Seizure (1430.03)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
3:00			3:00

DESCRIPTION:

Although the legal requirements of a proper search and seizure are the same in a computer environment as for any other, the law enforcement officer is certain to encounter unconventional legal situations when a computer, or computer related paraphernalia, is a part of the search environment. This course examines the structure of the Fourth constitutional Amendment and the impact it will have on the law enforcement officer in the nature of redefining the scope of the search, identifying items to be seized, and the nature of individual privacy in the context of an automated environment.

TERMINAL PERFORMANCE OBJECTIVE:

Given a graded practical exercise involving the execution of a search warrant, the student will demonstrate knowledge of how the Fourth Constitutional Amendment applies to computer environments of a dwelling or office and what may be searched and seized there.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify areas where the Fourth Constitutional Amendment applies to computer environments of a dwelling or office.

2. Identify the general provisions of the Fourth Constitutional Amendment as it relates to an individual's and a corporations right to privacy.

3. Identify the particularity requirements of the Fourth Constitutional Amendment regarding the description of the evidence to be listed on the affidavit and the warrant.

4. Identify what items may be searched and seized during the execution of a search warrant in a computer environment.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Electronic Communications (ECPA) Privacy Act of 1986 (1376.01)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
1:00			1:00

DESCRIPTION:

The Electronic Communications Privacy Act of 1986 is the result of Congress' attempt to better define privacy issues in the face of advanced communications technology. The provisions of the Act have a profound impact on how law enforcement officers conduct telecommunications investigations and the Act has more narrowly defined the government's power in such investigations. This course examines the provisions of the Act with the emphasis on classifying to the officer the parameters of authority as defined and modified by the Act.

TERMINAL PERFORMANCE OBJECTIVE:

Given a graded case investigation practical exercise, the student will demonstrate knowledge of the provisions of the Electronic Communications Privacy Act as it relates to any investigation, especially one involving communications technology.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify several reasons for the enactment of the Electronics Communications Privacy Act of 1986.

2. Identify the general provisions of the Electronic Communications Privacy Act.

3. Identify an electronic communications as defined by the Electronic Communications Privacy Act.

4. Identify the legal requirements for intercepting electronic communications and for obtaining stored communications.

5. Identify several ways in which investigative techniques in communications related investigations have changed since the enactment of the Electronic Communications Privacy Act.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Computer Viruses (3226.01)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
:30	:30		1:00

DESCRIPTION:

Computer viruses are maliciously modified computer programs that will, when undetected, destroy data on a computer system. Each year millions of computers in the United States are found infected with computer viruses and the damages inflicted can be and frequently are enormously destructive. Seized computer systems also have the potential of containing computer viruses. If programs or data files containing viruses are copied to another computer system, there is the potential of infecting that computer system. This course discusses computer viruses, what they are and how they work, how they can be detected and neutralized, and how contamination can be prevented.

TERMINAL PERFORMANCE OBJECTIVE:

Given oral questions, a laboratory exercise, an IBM compatible microcomputer, and a commercially available virus detection program, the student will define the dangers posed by and the protective methods available against computer viruses, and the student will analyze a computer for presence of a virus.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify the characteristics of a computer virus and its effect on a microcomputer system.

2. Identify various ways in which computer viruses are spread from one microcomputer to another.

3. Use a computer program to scan a diskette and a hard disk of a computer system for the presence of a virus.

4. Use and install various virus scanning computer programs onto a "sterile" boot diskette which will be used to boot a seized computer system and scan the computer system for viruses before copying data from it to tape drives, external disk drives or another computer system.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Computer File Encryption / Decryption (3430.02)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
1:00		1:00	2:00

DESCRIPTION:

Advancing computer technology, coupled with a growing user awareness of privacy and security issues, has resulted in the widespread use of program, electronic mail, and data file encryption techniques. Today, seemingly all sophisticated applications have their own optional encryption schemes including, WordPerfect, Lotus, Excel, and a host of others. The computer investigator can expect to encounter encrypted (and, therefore, unreadable) files when examining seized computer evidence. This course demonstrates software tools which will enable the student to decrypt many different files, and examines features of the most commonly used encryption/decryption tool used today: PGP.

TERMINAL PERFORMANCE OBJECTIVE:

Given a computer and files employing a variety of encryption techniques, the student will, utilizing software provided in class, determine what encryption scheme is used for each file, determine the password used to encrypt each file, and then decrypt each file using the appropriate password or key.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify which of the most popular commercial applications make use of encryption technology and describe the generally held opinions of the effectiveness of each.

2. Generally describe the Data Encryption Standard (DES) and its role in the world of computer security.

3. Generally describe the principals of the newly implemented "dual key" systems and their evolving role in the world of computer security.

4. Using a computer, work files and the PGP encryption program provided in class, install the PGP computer program, create the keys, save the public key to a file, and, working with a partner, encrypt and decrypt files.

5. Identify steps to take in an investigative activity when encrypted files are found and the password can not readily be determined by the investigator.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: File Compression (3436.01)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
:30	:30		1:00

DESCRIPTION:

With the advanced speeds of communication, and the increased popularity of the Internet as an information resource comes the need to store more information in a smaller amount of space, especially for uploads and downloads to and from the Internet. Knowledge of the concepts governing file compression programs is essential for accessing information through the Internet. Experience with the use of at least one kind of file compression program will also greatly assist the investigator who is attempting to obtain information relevant to an investigation through seizure of computer data. This course introduces the participant to file compression programs and their typical functions.

TERMINAL PERFORMANCE OBJECTIVE:

Given several laboratory exercises, an IBM compatible microcomputer, and a commercially available file compression program, the student will identify the characteristics of a data file created by the file compression program, use the computer program to compress and uncompress information, and identify methods used to identify files compressed on a seized computer system.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify the characteristics of a compressed file and methods that can be used to identify a compressed file within data files and fragments from a seized computer system.

2. Use a computer program to compress and uncompress data.

3. Identify and use practical options available within file compression programs.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Hardware Laboratory (3431.02)

LENGTH OF PRESENTATION:

<u>LECTURE</u>	<u>LABORATORY</u>	<u>PRACTICAL EXERCISE</u>	<u>TOTAL</u>
:30	:30		1:00

DESCRIPTION:

This course, requiring the use of a tool kit provided for training, requires the participant to disassemble a personal computer, examine, inventory, and optionally photograph the interior, reassemble, and return the computer to operation. Upon completion of the exercise, the student will be able to recognize the various components of a computer and determine the operational capabilities of the system.

TERMINAL PERFORMANCE OBJECTIVE:

Given a tool kit, a fully functional personal computer with keyboard and monitor, and both verbal and written instructions, the student will disassemble the computer and inventory the interior components, reassemble the system and restore the computer to operation in the classroom.

INTERIM PERFORMANCE OBJECTIVES:

1. Given a personal computer, identify the type of system and the obvious external physical characteristics.

2. Given a set of oral and written instructions, and a tool kit, disassemble the computer by:

   a. removing electrical power from the computer and peripheral devices;

   b. neutralize static electricity by touching a grounded piece of metal on the computer;

   c. removing the screws securing the computers case and disattaching the case;

   d. removing all plug-in circuit boards installed in the computer;

   e. removing all disk drives and controller cards.

3. Inventory the equipment by recording names, serial numbers, and identifying characteristics of each component.

4. Reversing the order in Interim Objective #2, reassemble the computer and replace the case.

5. Re-attach all peripheral devices, connect power lines, and turn the computer on.

6. Check computer operability by observing the appropriate operating system prompt.

7. In case computer fails to operate normally, determine the cause of failure.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: DISK ANALYSIS: Miscellaneous Investigative Utilities (3221.04)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
1:00	4:00	3:00	8:00

DESCRIPTION:

This course introduces training participants to utility programs provided with commercial software packages, created by law enforcement officers, and marketed as public domain/shareware to conduct investigative analysis on magnetic media. The four previous Disk Analysis courses have introduced the concepts these utilities are based on, and have shown the use of two Norton Utility programs: DISKEDIT and UNERASE. The remainder of the Norton Utility programs are demonstrated during this course, some of which are recommended for use during an investigative analysis, others are not. Investigative utilities created by law enforcement officers from various agencies are also demonstrated and used. During a final practical exercise, students use information received within the context of the Case Investigation to recover information from diskettes and from seized computer systems/data.

TERMINAL PERFORMANCE OBJECTIVE:

Given an investigative scenario(s) and an IBM compatible Microcomputer, the student will recover data pertinent to the investigation from a diskette using various investigative utilities.

INTERIM PERFORMANCE OBJECTIVES:

1. Use various Norton Utility programs to locate data related to an investigation on a diskette.

2. Use various utility programs created by law enforcement officers to identify relevant investigative information on a diskette.

3. Use public domain/shareware utility programs to find data on a diskette.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Local Area Network (LAN) Seizure and Analysis (3234.04G)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
4:00			4:00

DESCRIPTION:

If law enforcement officers execute a search warrant in a business environment for anything that can be written or typed, chances are that the seizure of computer data is within the scope of the search warrant. In fact, the computer system is often one of the targets of the search. In a business environment, multi-user systems are often prevalent. To extract data from a multi-user system requires a more advanced degree of knowledge than to retrieve data from a DOS, stand-alone IBM-compatible computer system. This course discusses configurations of Local Area Networks, specifically networks driven by the Novell operating system, and examines seizure and analysis procedures.

TERMINAL PERFORMANCE OBJECTIVE:

Given an investigative scenario, the student will discuss terminology and configurations for Networks, develop an investigative plan for the seizure of the appropriate "parts" of a Local Area Network and associated hardware/software, and define some of the System Management programs available for device/volume/file management on a Novell Netware Operating System, and to appropriately recover data from the computer system while preserving the authenticity and integrity of the seized data.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify the types of modern networks that exist today.

2. Define the major characteristics of networks.

3. Define several topology configurations of networks.

4. Identify several investigative considerations during the planning phase of Executing a Search Warrant in a Networked Environment.

5. During a simulated investigative seizure of a LAN, list methods that may be used to access the system manager/superuser password on a Novell server.

6. During a simulated investigative seizure of a LAN, define the commands to access the main menu of a Novell server, and what menu options may be most helpful.

7. During a simulated investigative seizure of a LAN, describe some of the steps that may be taken to take control of the computer system, and to search/recover files from the system.

8. During a simulated investigative seizure of a LAN, describe procedures to take to only seize the data from a LAN computer system configuration.

METHOD OF EVALUATION: Completion of course.

COURSE TITLE: Investigative Techniques in Computer Related Investigations (3207.04)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
2:00	1:00	1:00	4:00

DESCRIPTION:

This course relates various innovative as well as traditional investigative techniques to be used in computer criminal investigations. Topics discussed include types of evidence encountered, protecting evidentiary integrity, and preparing for and executing search warrants in computer environments. Also discussed during this course are considerations during the preparation process to Executing a Search Warrant in an Automated Environment. These considerations include creating a boot disk to perform a cursory analysis of the computer system. Subsequent to this course, and employing the principles discussed here, the participant will participate in an execution of a search warrant practical exercise.

TERMINAL PERFORMANCE OBJECTIVE:

Given a case study and a case investigation practical exercise involving a simulated computer related crime, the participant will demonstrate a knowledge of legal and operational principles in computer related searches.

INTERIM PERFORMANCE OBJECTIVES:

1. List five considerations in the preparation of an Affidavit for a Search Warrant when a computer facility is involved in a search.

2. Using the model Affidavit for Search Warrant, as presented in class, identify the appropriate legal and technical terminology to be used in the affidavit when a computer facility is involved.

3. Identify several ways in which the execution of a search warrant in a computer environment will vary from the traditional execution of a search warrant.

4. List several considerations that must be addressed during the planning phase of a computer search and seizure.

5. Identify appropriate procedures for officers to follow when entering the site of the execution of a search warrant.

6. List several actions that must be taken in a computer related search to ensure the integrity of the seized magnetic and electronic media.

7. Customize a boot disk with appropriate programs for preserving the integrity of the data on the seized computer system and for performing a cursory analysis on site.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Backing Up, Restoring, and Analyzing Seized Computer Systems/Data (3224.04)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
:30	1:00	2:30	4:00

DESCRIPTION:

This course relates various innovative techniques to be used during the seizure of a computer system or its data, including discussions on backup strategies, and three alternatives to seizing computers/data from a search site. Various backup devices are demonstrated, and students perform a practical exercise in backing up and restoring computer systems in the classroom. The course concludes with the creation of a set of guidelines to be used when backing up data from a seized computer system and restoring the data to another computer systems hard disk. Then the discussion turns to the actual analysis of the data. The principles taught within the first week of training, relating to the examination of diskettes, also apply here. But an additional consideration is that this computer system has not only files, but programs that control the working environment. Those files may need to be analyzed as well.

TERMINAL PERFORMANCE OBJECTIVE:

Given a case study and a continuing case investigation practical exercise involving a simulated computer related crime, the participant will backup data from seized computer systems using a variety of different devices and software, restore that data to another computer system for analysis, and perform a preliminary analysis of the programs controlling the configuration and overall environment of the computer system.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify three options that officers have in seizing storage media at a computer related search site.

2. Identify and use software and equipment that may be used to image computer systems hard disks seized or at a search site.

3. View previously created boot disk(s) to ensure it is configured properly, and identify appropriate programs to be placed on an external drive disk for possible analysis on site and during post seizure analysis.

4. Identify and analyze files and information within those files that may provide important configuration data and leads toward locating information valuable to the investigation.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Execution of a Search Warrant in an Automated Environment Practical Exercise (3222.02)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
		2:00	2:00

DESCRIPTION:

One of the most important elements in a criminal investigation, and one of the most potentially destructive if done incorrectly, is the execution of a search warrant. Difficulties are compounded in a computer related search because of the technology involved. If equipment is mismanaged or mishandled, or not labeled correctly, the consequences could be devastating. This practical exercise enables the participants to plan and execute a search in a computer environment applying the principles learned in previous training courses, and employing techniques for seizing technological equipment presented within this training program. Students will be required to seize data from computer systems at the search site by performing a mirror image backup of the data on the computer system, and later restore the data to another computer system and analyze the data.

TERMINAL PERFORMANCE OBJECTIVE:

Given a practical exercise involving a suspected, automated crime scene, the student, working as a team member, will execute an approved search warrant, conduct an effective, legal computer-related search, and seize and backup computer-related equipment and/or data specified in the search warrant affidavit.

INTERIM PERFORMANCE OBJECTIVES:

1. Initiate the appropriate steps and acquire the appropriate equipment and software in preparing for the execution of a search warrant in an automated environment.

2. Use appropriate procedures to conduct a thorough and legal search in keeping with the scope of the approved search warrant.

3. Perform a mirror image backup of the computer system(s) containing data to be seized.

4. Inventory, secure and appropriately transport seized items from the search site.

METHOD OF EVALUATION: Demonstrated proficiency.

COURSE TITLE: Prosecution Considerations in Computer-Related Crime Investigations (3215.02)

LENGTH OF PRESENTATION:

LECTURE	LABORATORY	PRACTICAL EXERCISE	TOTAL
2:00			2:00

DESCRIPTION:

This course is designed to introduce the participant to various problems encountered in the prosecution of computer-related crimes of which the investigator should be aware. Lecture, participant questions, and discussions are used to explore these problems and suggest means of working within the limitations and constraints of these problems in order to enhance the possibility for more effective government presentations in computer-related prosecutions.

TERMINAL PERFORMANCE OBJECTIVE:

Given a series of oral questions from the instructor, the participant will identify various problems inherent in the prosecution of computer-related crimes and the role of the investigator both during the investigation and as a witness during the prosecution in the light of these problems.

INTERIM PERFORMANCE OBJECTIVES:

1. Identify differences between the traditional relationship of the prosecutor and investigator and the relationship that should exist between the two in a computer-related prosecution.

2. Identify factors relating to evidence that make the prosecution of computer crimes unique from the prosecution of other types of crimes.

3. Identify considerations which affect the establishment of venue in computer-related prosecutions.

4. Identify problems encountered in charging the crime in computer-related prosecutions.

5. Identify factors to consider when choosing an expert witness in computer-related prosecutions.

6. Identify the effect of the "standing to object" question and how it can be used in computer prosecutions.

7. Identify the advantages and disadvantages of civil and administrative proceedings as alternate remedies to criminal prosecution.

8. Identify various types of visual aides and demonstrations that can be used to make an effective prosecution presentation.

METHOD OF EVALUATION: Completion of course.

Course Information
PROGRAM OF INSTRUCTION

Course			Hours of Instruction	
			Practical	
	Lecture	Lab	Exercises	Total
Disk Analysis: DOS/Batch Files	2:00	2:00	2:00	6:00
Disk Analysis: Windows/File Viewers	:30	1:30	2:00	4:00
(note: two hours of this course is conducted after hours)				
Disk Analysis: DOS/Batch Files and Windows/File Viewers PE			2:00	2:00
Disk Analysis: Boot Process and Configuring a Boot Disk	2:00	1:00	1:00	4:00
Disk Analysis: Recovering Erased Data from Disks	4:00	6:00	8:00	18:00
Disk Analysis: Final PE			5:00	5:00
Computer Search and Seizure	3:00			3:00
ECPA 1986	1:00			1:00
Computer Viruses	:30	:30		1:00
Computer File Encryption/ Decryption (PGP)	1:00		1:00	2:00
File Compression	:30	:30		1:00
Hardware laboratory		2:00		2:00
Miscellaneous Investigative Utilities	1:00	4:00	3:00	8:00
Local Area Network Seizure and Analysis	4:00			4:00
Investigative Techniques in Computer Related Investigations	2:00	1:00	1:00	4:00
Backing Up, Restoring and Analyzing Seized Computer Systems/Data	1:00	:30	2:30	4:00
Execution of a Search Warrant in an Automated Environment PE			2:00	2:00
Prosecution Considerations in Computer Related Crime Investigations	2:00			2:00
Subtotal	24:30	19:00	29:30	73:00

Administrative Time:

Introduction/Orientation	4:00
Critique/Graduation	1:00
SUBTOTAL	5:00

TOTAL PROGRAM LENGTH:

Lecture:	24:30
Laboratory:	19:00
Practical Exercise:	29:30
Administration	5:00
TOTAL	**78:00**

Sample Schedule

The following is a sample schedule for the

CRIMINAL INVESTIGATIONS IN AN AUTOMATED ENVIRONMENT TRAINING PROGRAM (CIAETP)

FEDERAL LAW ENFORCEMENT TRAINING CENTER

CRIMINAL INVESTIGATIONS IN AN AUTOMATED ENVIRONMENT

MASTER SCHEDULE

Room:

Week One

Coordinator: Ms. Schaffer

	Monday	Tuesday	Wednesday	Thursday	Friday
7:30 - 8:30	Introduction/Orientation *(3210.02)* *Ms. Schaffer*	Disk Analysis: Review, DOS/Batch Files (Cont'd) *FFI*	Disk Analysis: Boot *(3229.03)* FFI	Disk Analysis: Recovery of Erased Data *(Cont'd)* *FFI*	Disk Analysis: Recovery of Erased Data (Cont'd) *FFI*
8:30 - 9:30					
9:30 -10:30	Pre-Test: Laptop Issue *(3204.02)* *Ms. Schaffer*	Computer Viruses *(3226.01)* *FFI*			
10:30 -11:30		File Compression *(3436.01)* *FFI*	Hardware Inventory Lab *(3433.02)* *FFI*		
11:30 -12:30	#####	#####	#####	#####	#####
12:30 - 1:30	Disk Analysis: Review, DOS/Batch Files *(3232.06)* *FFI*	Disk Analysis: Windows, File Viewers *(3231.02)* *FFI*	Hardware Inventory Lab *(3433.02)* *FFI*	Disk Analysis: Recovery of Erased Data *(Cont'd)* *FFI*	Continuing Case Invest.: Practical Exercise *(3216.02)* *FFI*
1:30 - 2:30			Disk Analysis: Recovery of Erased Data *(3228.18)* *FFI*		Disk Analysis: Recovery of Erased Data *(Cont'd)* *FFI*
2:30 - 3:30		Disk Analysis: DOS Files/ Viewers *PE (3218.02)* *FFI*			
3:30 - 4:30					
Afterhrs	Disk Analysis: Viewers *(3231.02)* *FFI*	MS-DOS Commands Review *FFI*		Disk Analysis Laboratory *FFI*	Saturday: Disk Analysis Lab *FFI*

FEDERAL LAW ENFORCEMENT TRAINING CENTER
CRIMINAL INVESTIGATIONS IN AN AUTOMATED ENVIRONMENT

MASTER SCHEDULE

Room:

Week Two

Coordinator: Ms. Schaffer

	Monday	Tuesday	Wednesday	Thursday	Friday
7:30 - 8:30	Continuing Case Invest. (½) Computer Related Statutes *(1060.03)*	Continuing Case Invest. (½) Computer Search and Seizure *(1430.03)*	Investigative Techniques *(3207.04)*	Execution of Computer Search Warrant *(3222.02)* Group A	Continuing Case Invest. *(Cont'd)* *FFI*
8:30 - 9:30				Computer Encryption - Decryption *(3430.02)* Group B	Prosecuting Attorney Presentation *(3215.02)*
9:30 -10:30		*LGD*		Execution of Computer Search Warrant *(3222.02)* Group B	*Guest*
10:30 -11:30	Computer Evidence *(1050.01)* *LGD*	ECPA/1986 *(1376.01)* *LGD*	*FFI/Guest*	Computer Encryption - Decryption *(3430.02)* Group A	Graduation/Closure *(3210.01)* *FFI*
11:30 -12:30	#####	#####	#####	#####	#####
12:30 - 1:30	Disk Analysis: Misc. *(3221.04)*	Local Area Networks: and Analysis *(3234.04G)*	Backup, Restore, Analysis of Seized Data *(3224.04)*	Disk Analysis: Final PE *(3233.04)*	
1:30 - 2:30					
2:30 - 3:30					
3:30 - 4:30	*FFI*	*FFIGuest*	*FFI/Guest*	*FFIGuest*	
Afterhrs		Investigations on the *FFI/Guest*	Cont. Case Invest. PE *(Cont'd)* *FFI*	Disk Analysis: Final PE *(Cont'd)* *FFI*	